UNITED STATES DISTRICT COURT
DISTRICT OF VERMONT

IN THE MATTER OF THE SEARCH OF:
92 OVERLAKE PARK
APARTMENT 2
BURLINGTON, VERMONT

Case No. 2:19-MJ-88

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Caitlin Moynihan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 92 Overlake Park, Apartment 2, Burlington, Vermont (hereinafter the "Subject Premises"), further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with Homeland Security Investigations (HSI). HSI is a directorate within Immigration and Customs Enforcement (ICE). ICE is a subordinate component of the Department of Homeland Security (DHS) and the successor to many of the law enforcement powers of the former Immigration and Naturalization Service and the former U.S. Customs Service. I have been a Special Agent since October 2009. I graduated from the Federal Law Enforcement Training Center in April 2010. I am currently assigned to the Burlington, Vermont Residence Office. I hold a Bachelor of Arts degree in sociology from Providence College. Throughout my time with HSI, I have gained experience, through training and everyday work, in investigating violations relating to child exploitation and child pornography.

3. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. I know that Title 18, United States Code, Section 2252(a)(4)(B) prohibits a person from possessing images of children engaged in sexually explicit conduct, as defined in 18 U.S.C. section 2256 ("child pornography"), Section 2252(a)(1) prohibits the transportation of child pornography, and 18 U.S.C. Section 2252(a)(2) prohibits the receipt and distribution of child pornography.

4. I believe that probable cause exists to believe that property which constitutes evidence of the following crimes: possession, transportation, receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A, may be found inside the premises at 92 Overlake Park, Apartment 2, in Burlington, Vermont (the Subject Premises), as further described in Attachment A.

5. The property sought to be seized and searched is described in Attachment B.

6. I have not included in this affidavit every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to issue a warrant to search the Subject Premises.

7. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement officers and witnesses, and on my experience and training as a Special Agent.

CHARACTERISTICS OF CHILD PORNOGRAPHERS

8. Based upon my knowledge, experience, and training in child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to many individuals involved in such crimes:

a. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child-pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, or in some other secure location.

d. Likewise, those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area.

e. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with others to share information and materials.

BACKGROUND OF INVESTIGATION

9. Based upon my knowledge, experience, and training in child exploitation investigations, and the training and experience of other law enforcement officers with whom I have consulted, I know the following about peer-to-peer (P2P) file sharing:

a. P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. To use P2P file sharing, a user must first obtain the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running the same or compatible P2P software. To obtain files on the network, a user opens the P2P software on the user's computer and conducts a search for files currently being shared on the network. The results of a search are displayed to the user. The user then selects file(s) from the results for download.

b. For example, a person interested in obtaining images of child pornography would open the P2P application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects, from the results displayed, the file(s) he/she wants to download. The downloaded file is stored in the area previously designated by the user and/or the software. The downloaded file will remain until moved or deleted.

c. One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. The advantage of this is that it speeds up the time it takes to download the file.

d. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address is unique to a particular computer during an online session. The IP address provides a unique location, making it possible for data to be transferred between computers.

e. The computer running the file sharing application has an IP address assigned to it while it is on the Internet. Computer users are able to see the IP address of computers sharing files on P2P networks.

10. Based on my training and experience, which includes experience investigating child exploitation cases, as well as my participation in a two-day training sponsored by the Internet Crimes Against Children task force on the use of the BitTorrent peer-to-peer network to facilitate investigations into users of the BitTorrent network, and the training and experience of the law enforcement personnel with whom I have spoken, I know the following about the BitTorrent file sharing network:

a. P2P file sharing networks, including BitTorrent, are frequently used to trade digital files of child pornography. These files include both still image and movie files.

b. To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used for the purpose of sharing digital files. Some examples are: uTorrent, Shareaza and BitLord.

c. It is the computers linked together through the Internet using this software that form the BitTorrent network that allows for the sharing of digital files between users. Most computers that are part of this network are referred to as "peers" or "clients."

d. During the installation of typical "BitTorrent" software, various settings are established which configure the host computer to share files. Depending upon the BitTorrent program used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to other BitTorrent users to download.

e. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which

maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network, a process referred to as "seeding."

f. To share a file or a set of files on the BitTorrent network, a "Torrent" file needs to be created by the user that initially wants to share a file or set of files. A Torrent is typically a small file that describes the file or files that are being shared, which may include information on how to locate the file(s) on the BitTorrent network. A typical BitTorrent program will have the ability to create a Torrent file. It is important to note that the Torrent file does not contain the actual file(s) being shared, but only information about the file(s) described in the Torrent, such as the name(s) of the file(s) being referenced in the Torrent and the "info hash" of the Torrent. The info hash is a SHA-1 hash value[1] of the set of data describing the file(s) referenced in the Torrent, which include the SHA-1 hash value of each file piece, the file size, and the file name(s). When another user (peer/client) later receives a particular piece, the hash of the piece is compared to the recorded hash to test that the piece is error-free.

g. Multiple persons sharing the same file(s) can deliver different pieces of the file(s) to the BitTorrent software on the downloading computer. BitTorrent software can only succeed in reassembling the pieces obtained from different users correctly if the individual pieces are exactly the same (digitally identical). The BitTorrent program does this by matching the exact SHA-1 piece hash described in the Torrent file. Accordingly, the BitTorrent software can ensure that a complete and exact copy can be reconstructed from the parts.

h. Once a Torrent is created, in order to share the file(s) referenced in the Torrent file, a user typically makes the Torrent available to other users, such as via websites on the Internet.

---

[1] SHA1 hash values are obtained by applying a one-way mathematical algorithm to a digital file, of any length, to produce a fixed length output hash value. The resulting hash value is a unique and extremely compact alphanumeric representation of that file. Hash values are also known as digital signatures and are used in integrity protection and evidence verification in electronic discovery and computer forensics. It is computationally infeasible to find two different files which produced the same hash value when run through the above-referenced one-way mathematical algorithm.

i. For a typical user to locate Torrent files of interest and download the files that they describe, they use keyword searches on torrent indexing websites, historical examples of which include isohhunt.com and thepiratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate Torrent files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by Torrent files, only the Torrent file. Once a Torrent file is located on the website that meets a user's keyword search criteria, the user will download the Torrent file to their computer. The BitTorrent program on the user's computer will then process that Torrent file in order to find users (peers/clients) on the network that have all or part of the file(s) referenced in the Torrent file.

j. The actual file(s) referenced in the "Torrent" are obtained directly from other users (peers/clients) on the BitTorrent network. This means the download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) sharing the actual file(s) (not the torrent file but the actual files referenced in the .torrent file using any BitTorrent client.). Once completed, the downloaded file is then stored in the area previously designated by the user and/or the program. The downloaded file(s), including the torrent file, will remain until moved or deleted.

k. For example, a person interested in obtaining child pornography would open a torrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user selects a Torrent file from the results. This Torrent file represents the files the person wants to download. Once the Torrent file is downloaded, it is then used by a BitTorrent program which the user would have previously installed. The Torrent file is the set of instructions the program needs to find the files referenced in the Torrent file. The files are then downloaded directly from the computer or computers sharing the file.

l. In the BitTorrent network, a "computer" could be a laptop or desktop computer, or it could also be a smart phone or tablet or other electronic device.

m. Even though the BitTorrent network links together computers all over the world and users can download files, it is not possible for one user to send

or upload a file to another user of the P2P network without the receiving party's active participation. The software is designed only to allow files to be downloaded that have been selected for download by the receiver. It is impossible to send files from one computer to another without the receiver's permission or knowledge.

PROBABLE CAUSE

11. On March 25, 2019, I was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. I initiated an investigation for a device at IP address 98.229.2.46 because it was associated with a torrent with the infohash: 32b58a925d17918f26a8159bce427c1e41458793. This torrent references one file which has been identified as being a file of investigative interest to child pornography investigations. Files of investigative interest are files that have been previously identified by law enforcement officers as files containing child exploitative material based on their SHA values.

12. Using a computer running investigative BitTorrent software, I directly connected to the device at IP address 98.229.2.46. The user's BitTorrent software reported itself as: -UM1870- µTorrent Mac 1.8.7.

13. On Monday, March 25, 2019, between 1343 and 1434 EDT hours, I downloaded one incomplete file that the device at IP address 98.229.2.46 was making available. I have viewed this file and consider it to contain child pornography.

a. The device at IP address 98.229.2.46 was the sole candidate for the download, and as such, the file was downloaded directly from IP address 98.229.2.46.

b. The file is described as follows:

"1st-Studio Siberian Mouse HD_125 (M-11).wmv"– This is a video file 18 minutes and 41 seconds in length. Only portions of the video play. This video depicts two nude pubescent female children, approximately 12-14 years old, on what appears to be a bed. Throughout the video,

> one girl performs oral sex on a dildo, while the other girl appears to be touching her genital area with a vibrator. There is no visible pubic hair on either pubescent child and each child has minimal breast development.

14. On or about March 26, 2019, I searched publicly available records located online and determined that 98.229.2.46 was assigned to a company known as Comcast Cable Communications, LLC. (Comcast).

15. On April 10, 2019, I served a subpoena on Comcast via fax for subscriber information for IP Address 98.229.2.46 assigned on March 25, 2019 at 14:34 EDT, to include 180 days of IP address history. On April 11, 2019, the below information was received from Comcast Legal Response Center regarding the subscriber of IP address 98.229.2.46 at the above date and times as:

Subscriber Name:	SEAN FIORE
Service Address:	92 OVERLAKE PARK APT 2 BURLINGTON, VT 054014012
Telephone #:	(802) 734-5216
Type of Service:	High Speed Internet Service
Account Number:	8773500210892560
Start of Service:	1/19/2018
Account Status:	Active
IP Assignment:	Dynamically Assigned
IP History:	See attached to date of Subpoena
E-mail User Ids:	sean.fiore (the above user ID(s) end in @comcast.net)

16. I sent a request to the Vermont Intelligence Center (also known as the Vermont Fusion Center) for information on Sean Fiore. Based on my training and experience, I know that the Fusion Center provides accurate and timely strategic intelligence products to assist agencies with criminal cases, including but not limited to background intelligence on persons suspected of criminal activity, timelines, and link charts to assist in organizing a case. The Fusion Center

response indicated that Sean Fiore was born in 1983. I conducted record checks in the FBI Interstate Identification Index (III) and in the State of Vermont criminal history databases for Sean Fiore, which yielded negative results.

17. On April 12, 2019, I checked with the United States Postal Service (USPS) to ascertain who was currently receiving mail at the Subject Premises. A response was received indicating the following names are receiving mail at the Subject Premises: Lillian Kimball, Mara Coven, Sean Fiore, and Aude Fiore.

18. On April 12, 2019, I contacted the Vermont Department of Motor Vehicles (DMV) and asked for registered vehicles and drivers associated with the Subject Premises. The response from DMV indicated approximately seven (7) individuals were associated with the Subject Premises at one time, to include the four names provided by the USPS. Additional record checks on the other three names revealed these individuals no longer appear to reside at the Subject Premises. The DMV response further revealed the following:

a. Mara Coven had the following vehicle registered to her: a 2007 Volvo XC7, silver in color, bearing Vermont tag: FPD723. I also received a DMV photograph of her.

b. Lillian Kimbell had no vehicles registered to her. I received a DMV photograph of her.

c. Aude Fiore had no vehicles registered to her. I received a DMV photograph of her.

d. Sean Fiore had the following vehicle registered to him: a 2015 Volkswagon Golf, silver in color, bearing Vermont tag: FRY588. I received a DMV photograph of him.

19. On April 17, 2019, I caused a summons to be sent to the Vermont Department of Labor requesting wage information related to Sean Fiore with SSN: XXX-XX-9757. I received the response on April 19, 2019. The response indicated that as of quarter three in 2018, Sean Fiore was employed by UVM Nursing and Health Sciences; which was also referred to as Practice Group, Inc.

20. An open source check of Google for "Sean Fiore University of Vermont" revealed two results of interest.

a. One was a website for UVM Medical Center with a blog on "Understanding the New Blood Pressure Guidelines." This article was dated March 23, 2017 and in the references section, the following was listed, "*Sean Fiore, MS, RN – Sean is a Primary Care Nurse who is currently pursuing his Doctorate in Nursing Practice – Adult-Gerontological Nurse Practitioner concentration at the University of Vermont. His interests in wellness stems from the belief that nurses ought to spend as much energy promoting wellness in the healthy as they do caring for the sick. Outside of work and school, he enjoys traveling and cooking.*"

b. A second result was an article on a website for the UVM, College of Nursing and Health Sciences, titled "Work that Helps the World: Doctor of Nursing Practice Students Present Evidence-Based Practices." This article was published on April 2, 2019. The article contains a picture with the caption, "*Doctor of Nursing Practice students Sean Fiore (right), David Segel (left) and a friend celebrate the conclusion of project presentations.*" The male depicted on the right appears to match the previously obtained DMV photograph of Sean Fiore.

21. On April 16, 2019, the following investigative steps were taken:

a. At approximately 0610 hours, SA Mike McCullagh traveled to the Subject Premises. At this time, there were no lights observed on inside the residence. SA McCullagh observed a vehicle bearing Vermont tag: FRY588 parked in the driveway. Record checks revealed that this vehicle, a 2015 Volkswagon Golf, silver in color, is registered to Sean Fiore. No other vehicles were observed at the Subject Premises at this time.

b. At approximately 1534 hours, SA McCullagh and I traveled to the Subject Premises. We observed no vehicles in the driveway. I used an openly available wireless network discovery tool to search for available wireless networks while parked in front of the Subject Premises. The program identified approximately 66 wireless networks in the area, some of which appeared to be unsecured. There were no obvious network names associated with the Subject Premises. At this time, I took photographs of the Subject Premises.

c. The main entrance to the residence appears to be in the front of the residence, facing Overlake Park. On the side of the garage there is a door which resembles an apartment entrance door; the door is half glass with a door knocker on it. There is also a glass storm door and mailbox next to it. There is no number or markings near the door, which appears to enter into the garage area of the residence.

22. On April 23, 2019, I took the following investigative steps:

a. At approximately 1503 hours, I traveled to the Subject Premises. I did not see any vehicle associated with Sean Fiore in the driveway at this time.

b. I followed up with the USPS and asked if the carrier could indicate where Apartment 2 is located at the Subject Premises. A response was received on April 30, 2019, which stated, "According to the postmaster the apartment has not been approved by the town yet

so there is only one mailbox for the house which is located by the garage. All mail and packages are left there so they do not know which entrance is used to enter the Apartment."

23. I have spoken with SA McCullagh about his conversation with Bill Ward, the Director of Code Enforcement for the City of Burlington, about the Subject Premises. According to SA McCullagh, Mr. Ward indicated that the Subject Premises is a single-family residence and that there are currently no open permits to make it a multi-unit residence.

24. I searched the City of Burlington, Office of the City Assessor webpage for 92 Overlake Park. 92 Overlake Park is listed as a single-family home. The owner is listed as Mara L. Coven.

25. On May 8, 2019, Lieutenant Daniel Gamelin, of the Chittenden County Sheriff's Office, went to 92 Overlake Park, in Burlington, Vermont. While Lt. Gamelin was at the front of the residence he observed a male and a female come from the walkway along the left side of the garage to the residence, when facing the residence from Overlake Park. Lt. Gamelin recognized the male as Sean Fiore from his DMV photo. Lt. Gamelin spoke with both Fiore and the female. Lt. Gamelin learned that 92 Overlake Park has three apartments. When facing from Overlake Park, Fiore and the female live in the apartment to the far left, the landlord lives in the middle unit and there is an additional unit on the right. Lt. Gamelin also observed the male and female enter a vehicle, which was registered to Sean Fiore and depart the area.

26. I have viewed the Subject Premises and describe it here and in Attachment A as follows: a Cape Cod style home, white in color, with a dark grey shingled roof. The Subject Premises has two "doghouse" a.k.a. gable dormers attached to the roof area on the second floor. The number "92" is displayed to the left of the front door. When facing from Overlake Park,

there is a garage attached to the left of the residence, on the left side of the garage, there is an entrance door with a storm door. This is the entrance door to Apartment 2. The upper half of the entrance door has glass on it. There is also a door knocker attached to the center of the door; to the right of the door there is a mailbox attached to the side of the house.

TECHNICAL TERMS

27. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses. There are two commonly used types of IP addresses called IPv4 and IPv6. IPv4, or IP version 4, is a 32-bit numeric address that consists of a series of four numbers, each ranging between 0 and 255, that are separated by dots. An example of an IPv4 address is 123.111.123.111. IPv6, or IP version 6, is a 128-bit hexadecimal address that consists of a series of eight values separated by colons. Hexadecimal values consist of a series of numbers between 0 and 9 and letters between A and F. An example of an IPv6 address is: 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

d. "Child Pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the

visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

e. "Minor" means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

f. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

g. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have spoken, I know the following about computers and computer technology:

   i. Computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed. Basically, computers serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

   ii. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

iii. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store many thousands of images at very high resolution.

iv. The Internet affords individuals several different venues for meeting each other, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Individuals also use online resources to retrieve and store child pornography such as email services and cloud storage. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. I believe that there is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to view or share child pornography the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded

on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

33. Because several people share the Subject Premises as a residence, it is possible that the Subject Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

34. I submit that this affidavit supports probable cause for issuance of a warrant to search the Subject Premises, described in Attachment A, and to seize and search the items described in Attachment B.

35. I request authorization to electronically record the voices and conversations of any person present at the Subject Premises on the day of the execution of the search warrant. An identified police officer(s) will be a knowing and consenting party/parties to the participant

electronic monitoring. The participant electronic monitoring may include a digital recording made with the use of audio transmitting and receiving devices during contact with the persons mentioned above.

Respectfully submitted,

CAITLIN MOYNIHAN
SPECIAL AGENT

Subscribed and sworn to before me
on May 9, 2019:

HON. JOHN M. CONROY
UNITED STATES MAGISTRATE JUDGE